Integrate Reveal(x) 360 with CrowdStrike

Published: 2024-06-19

Integrate ExtraHop Reveal(x) 360 with CrowdStrike to provide increased visibility and control over your devices.

System Requirements

ExtraHop Reveal(x) 360

- Your user account must have privileges on Reveal(x) 360 for System and Access Administration or Cloud Setup.
- Your Reveal(x) 360 system must be connected to an ExtraHop sensor with firmware version 8.8 or later. Version 8.9 or later is required to enable the integration option for device containment.
- Your Reveal(x) 360 system must be connected to ExtraHop Cloud Services ⤴.

CrowdStrike

- You must have the security token provided by ExtraHop in your welcome email or your CrowdStrike API client ID, client secret, and endpoint.

  > **Note:** If you upgrade your ExtraHop system, you will need to enter new credentials to configure new integration options.
- The scope of the CrowdStrike API client must include READ permissions for Indicators (Falcon) to enable integration options for displaying links to CrowdStrike devices or CrowdStrike Falcon threat intelligence.
- The scope of the CrowdStrike API client must include READ and WRITE permissions for Hosts to enable the integration option for device containment.

Configure the CrowdStrike integration

1. Log in to the Reveal(x) 360 system.
2. Click the System Settings icon ⚙ and then click **Integrations**.
3. Click the CrowdStrike tile.
4. Choose one of the following options:

   - Click **Enter Security Token** if you received a token from ExtraHop when you signed up for a free trial.

     1. Paste the security token from your welcome email into the **CrowdStrike Security Token** field.
     2. Click **Connect**.
   - Click **Enter Client ID and Secret**.

     1. Enter your CrowdStrike client ID into the API Client ID field.
     2. Enter your CrowdStrike client secret into the API Client Secret field.
     3. Select your CrowdStrike API Region Endpoint from the drop-down list.
     4. Click **Test Connection** to ensure that the ExtraHop system can communicate with CrowdStrike Falcon.
     5. Click **Connect**.

        > **Note:** If you see a message that your credentials are invalid, re-type your client ID and secret and click **Connect** to try again.
5. Optional: Configure any of the following integration options:

> **Note:** The integration cannot import more than 50,000 total indicators from CrowdStrike.

- Select **Display links to CrowdStrike Falcon for threat intelligence**. Click links to view threat intelligence ⤢ in CrowdStrike Falcon.
- Select **Display links to CrowdStrike for devices that have Falcon software installed**. Devices must be local and have a MAC address. Links appear on the Device Overview page ⤢ for CrowdStrike devices.
- Select **Enable users to contain CrowdStrike devices from detections in Reveal(x) 360**. (Requires read and write access to Hosts). An option appears to initiate containment of CrowdStrike devices ⤢ that are participants in a security detection. Users must be granted access through the Detections Access Control global policy and have Full Write privileges or higher to initiate containment.

6. Click **Save**.